UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT CHATTANOOGA

UNITED STATES OF AMERICA,

Plaintiff,

v.

0.40401694 BITCOIN (BTC) SEIZED FROM BINANCE USER ID 36895141 (SUBJECT WALLET 1) IN THE NAME OF MARTINS EROMOSELE IYERE;

59,911.36 TETHER (USDT) SEIZED FROM BINANCE USER ID 20891886 (SUBJECT WALLET 2) IN THE NAME OF OLAWUMI STEPHEN ADEWALE; AND

9,128.847 TETHER (USDT), 1,346.37 DECENTRALAND (MANA), 1,039.6163 CURVEDAO (CRV), 14,690.894 ZILLQA (ZIL), 5.5550225 AVALANCHE (AVAX), 14,534,916 SHIBA INU (SHIB) SEIZED FROM BINANCE USER ID 18211927 (SUBJECT WALLET 3) IN THE NAME OF MOSES OLUMIDE SOKALE.

Defendant.

Case No. 1:23-CV- 218

Judges ________________

AFFIDAVIT IN SUPPORT OF VERIFIED COMPLAINT *IN REM*

I, Special Agent Jordan A. Foreman, being duly sworn, hereby declare as follows:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been

since January 2021. Prior to joining the FBI, I was a sworn Peace Office in the State of Indiana. As a general criminal detective, I have participated in numerous investigations involving violent crime, theft, extortion, threats, harassment, fraud, computer crimes, and internet-based crimes. As a detective I completed training in forensics for computers and mobile devices. I am currently assigned to the FBI Knoxville Cyber Task Force, and my duties include investigating computer related crimes. Due to my training, my experience, and this investigation, I am also familiar with the Internet, service providers, and the manner in which criminals use the Internet and computers to further their schemes. I have also attended FBI sponsored training and have had communications with law enforcement personnel who specialize in these areas. At all times during the investigation described herein, I have acted in my official capacity as Special Agent with the FBI.

2. Since the affidavit is being submitted for the limited purpose of a Verified Complaint *in Rem*, I have not included each and every fact known to me concerning this investigation. I only set forth the facts that I believe are necessary to establish probable cause for the issuance of these seizure warrants. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

3. The information contained in this affidavit is based on, among other things, my personal knowledge, and observations during the course of this investigation, information conveyed to me by the victim(s), the divisions of the FBI, the public, other government agencies and officials, law enforcement personnel, both domestic and foreign, and my review of records, documents and other evidence obtained during this investigation.

PURPOSE OF AFFIDAVIT

4. This affidavit is submitted in support of an application for a Verified Complaint *in Rem* for the following assets (collectively, the "**SUBJECT WALLETS**"):

a. 0.40401694 Bitcoin (BTC) Seized From Binance User ID 36895141, Martins Eromosele Iyere **(SUBJECT WALLET 1)**;

b. 59,911.36 Tether (USDT) Seized From Binance User ID 20891886, Olawumi Stephen Adewale **(SUBJECT WALLET 2)**; and

c. 9,128.847 Tether (USDT), 1,346.37 Decentraland (MANA), 1,039.6163 Curvedao (CRV), 14,690.894 Zillqa (ZIL), 5.5550225 Avalanche (Avax), 14,534,916 Shiba Inu (SHIB) Seized From Binance User ID 18211927 **(SUBJECT WALLET 3)**.

(Items a-c, together known as the "**SUBJECT WALLETS**")

5. As set forth below, I submit there is probable cause to believe that the SUBJECT WALLETS constitute proceeds from violations of Wire Fraud, 18 U.S.C. § 1343, and property involved in a money laundering transaction or money laundering conspiracy, in violation of 18 U.S.C. § 1956, or are traceable to such property. The SUBJECT WALLETS are, therefore, subject to forfeiture to the United States.

FORFEITURE AUTHORITY

6. The SUBJECT WALLETS are subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C), on the grounds that the funds contained in the above-listed accounts constitute proceeds that are directly traceable to violations of 18 U.S.C. § 1343 (Wire Fraud). The SUBJECT WALLETS are further subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(C) and 981(a)(1)(A), on the grounds that the funds contained in the above-listed wallets constitute proceeds that are directly traceable to violations of 18 U.S.C. § 1956 (Money Laundering). For reasons set forth below, probable cause exists for forfeiture of the SUBJECT WALLETS.

BACKGROUND ON CRYPTOCURRENCY

7. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

a. Cryptocurrency, a type of virtual and/or digital currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are ether, bitcoin, and Litecoin, etc. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[1] Cryptocurrency is not illegal in the United States.

b. Ether, "ETH", is a type of cryptocurrency. Payments or transfers of value made with ether are recorded in the Ethereum blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire ether through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange

[1] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

for fiat currencies or other cryptocurrencies), Ether ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by "mining." An individual can "mine" ether by using his/her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Ethereum transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it's not completely anonymous, Ethereum allows users to transfer funds more anonymously than would be possible through traditional banking and credit systems.

c. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key.") A public address is represented as a case-sensitive string of letters and numbers, 26–25 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key - the cryptographic equivalent of a password or PIN - needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

d. Although cryptocurrencies such as ether have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an oft used means of payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases. As of February 27, 2022, one ether is worth approximately $2,597.67 USD, though the value of ether is generally much more volatile than that of fiat currencies.

e. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code[2] with the public and private key embedded in the

[2] A QR code is a matrix barcode that is a machine-readable optical label.

code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase) or an API Key, as further explained below. I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

f. Ethereum "exchangers" and "exchanges" are individuals or companies that exchange ether for other currencies, including U.S. dollars. According to the Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.[3] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and/or the full bank account and routing numbers that the customer links to his/her exchange account. As a result, there is significant market demand for illicit

[3] *See* "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," *available at* https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

cryptocurrency-for-fiat currency exchangers, who not only lack AML or KYC protocols but often advertise their ability to offer customers stealth and anonymity. These illicit exchangers often exchange fiat currency for cryptocurrencies, such as by meeting customers in person or by shipping fiat currency through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9-10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1-2%).

g. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), investigators may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

h. Slippage refers to all situations in which a market participant receives a different trade execution price than intended. Slippage occurs when the bid/ask spread changes between the time a market order is requested and the time an exchange or other market-maker executes the order.

FRAUD INVESTIGATION BACKGROUND

8. Matthew McNulty (McNulty) resides in Cleveland, Tennessee 37311, where he engages in investing and trading in cryptocurrency assets. On February 10, 2021, McNulty completed a cryptocurrency token swap[4] through the server Anyswap, currently branded under the new name of Multichain. McNulty swapped the Ether cryptocurrency for another cryptocurrency, Fusion (anyFSN). Both cryptocurrency tokens operate on the Ethereum blockchain. However, during the transaction McNulty experienced slippage[5] of approximately $4,500 USD as the Fusion token devalued during the transfer.

9. On February 12, 2021, McNulty went onto the Telegram messaging application Anyswap exchange channel, where Anyswap users can communicate with each other, to seek help regarding the slippage. McNulty posted a public message in the chat and was contacted on Telegram by "Marcel" who was listed as an AnySwap (sic) Community Manager. However, the person McNulty communicated with was a scammer impersonating Marcel Cure, an actual community manager at Anyswap exchange. While a real 'Marcel' exists, the individual who

[4] Swapping refers to exchanging one coin or token for another.

[5] Slippage occurs when the bid/ask spread changes between the time a market order is requested and the time an exchange executes the order. Ex. A virtual token is purchased, and the price devalues between clicking to purchase the token and the transaction occurring on the blockchain. That loss of value is colloquially called slippage.

contacted McNulty was not actually Marcel. Rather, the person was an impersonation scammer with a profile that was almost identical to that of the real Marcel, the main difference being that the impostor's Telegram handle (akin to a user ID) was not the same. The impostor's Telegram handle is hidden.

10. The scammer directed McNulty to the website, https://walletconect[.]info, where McNulty entered the seed phrase[6] to his Metamask[7] cryptocurrency wallet. The website created a quick response code, QR code, which the scammer asked McNulty to screenshot and message to him. Shortly after sending the QR code containing his seed phrase, cryptocurrency tokens were removed from McNulty's Metamask wallet in the following amounts: 9999.93 LUNA tokens, 5256 Polkastarter tokens, 1898.1479 Injective tokens, and 0.296367 Ether tokens; all tokens operate on the Ethereum blockchain. The various virtual currencies were worth approximately $125,000 USD at the time they were stolen from McNulty and have since dramatically gained in value.

11. On March 24, 2021, the CipherBlade Blockchain Investigation Agency, a private company which specializes in blockchain forensics and tracking Bitcoin, Ethereum and other cryptocurrencies, created an Investigative report for McNulty at his request. In the report, Cipherblade listed the Internet Protocol (IP) address for the website https://walletconect[.]info as 169.255.59.74, with both the registrar and hosting provider for the website;

[6] Seed Phrase is a series of words generated by your cryptocurrency wallet that give you access to the crypto associated with that wallet. The seed phrase is similar to a master password to your wallet and operates much like a title to a car, in that once you have it, you own the car.

[7] MetaMask is a software cryptocurrency wallet used to interact with the Ethereum blockchain.

https://walletconect[.]info, being Web4Africa[8]. The March 24, 2021, CipherBlade report suggests the scammer(s) are based in Nigeria.[9]

12. The movement of the cryptocurrency taken from McNulty's Metamask wallet (0xC2017be9ec51efB88a1242dcE832a25D111166Aa) was tracked by open-source methods. Cryptocurrency was removed from McNulty's wallet and transferred, by a bad actor, to wallet 0xA75344CF46d3c1e287C6b0aaB02901455bF66899 **(Suspect Wallet 1)**. However, no property can be seized from this wallet because it is not associated with an exchange. From Suspect Wallet 1, the cryptocurrency was changed to other forms of cryptocurrencies and then transferred to multiple other wallets. My investigation revealed that some of those wallets are located on an exchange, specifically with Binance. I requested information from Binance and they provided Binance User Ids associated with each of the wallets in question.

13. In my training and experience, I believe that the SUBJECT WALLETS are conducting activity associated with money laundering. The pattern of withdrawals, transfers, and transactions is consistent with money laundering and attempts to conceal proceeds of fraud. Further, cryptocurrency is frequently used by criminals operating in the digital sphere as a medium of money laundering due to its pseudonymity and the perceived difficulties in tracing funds. It is common for money launderers to obtain Bitcoin and immediately convert the funds to another

[8] Web4Africa is an ICANN Accredited Domain Registrar & Web Hosting Company offering web hosting & domains from datacentres in South Africa, Ghana and Nigeria.

[9] IP Address: 105.112.150.218 (Lagos, Nigeria, Airtel Networks - not a VPN service). Date & Time: November 26, 2020 17:15:30 UTC and IP Address: 105.112.32.204 (Lagos, Nigeria, Airtel Networks - not a VPN service) Date & Time: August 8, 2020 16:31 UTC.

cryptocurrency, such as USDT, and to transfer to multiple other accounts in order to attempt to attempt to "wash" the money and hide illicit funds.

14. Following the flow of cryptocurrency, I discovered Wallet 0x41899a7213A848DC062F06bfb60578A9dd7E4D72 **(Suspect Wallet 2)** and believe it also belongs to the scammer. Ether token transactions were made from this wallet into McNulty's wallet in an attempt by the scammer to pay the transaction fees associated with removing/stealing the other cryptocurrency from McNulty's wallet. Seven substantial Ether transactions were completed between Suspect Wallet 1 and Suspect Wallet 2 just after the theft of cryptocurrency from McNulty's wallet.[10]

15. SUBJECT WALLET 1, Binance user ID 36895141, belonging to, or associated with, MARTINS EROMOSELE IYERE, is correlated with wallet address 0x7db1Eef5579C80F28020b79feef11056e3506E4A. This wallet received a large number of Tether tokens (6,100 USDT), from Suspect Wallet 2 on February 8, 2021, prior to the McNulty theft. Shortly after the McNulty theft, SUBJECT WALLET 1 received twelve (12) separate transactions, the first being on February 13, 2021 and the last March 8, 2021, from wallet 0x57b3d499FED2735A50Eb8f4f6B3aAD4bB6948114 (Intermediate Wallet 1) totaling an amount of 65.56890522771799 ETH (currently valued at approximately $225,226.57 USD). Intermediate Wallet 1 then received 18.872509413174878 ETH from Suspect Wallet 2 after the McNulty theft. This user Id is associated with an individual located in Nigeria.

16. SUBJECT WALLET 2, Binance user ID 20891886, belonging to or associated with, OLAWUMI STEPHEN ADEWALE, is correlated with wallet address

[10] There is no request for a seizure of Suspect Wallet 1, 2, or Intermediate Wallets because they are not associated with an exchange or under control of Binance.

0xE2abb7B6328Ff3f2Be3836434F95A5a554453df5. Subject Wallet 2 received 5.4286392498 ether in two transactions, on April 14 and April 21, 2021 respectively, from wallet 0xab55c83523ea8E6487Ad785dA5B88F9ceEdd9A6a (Intermediate Wallet 2), after the McNulty theft. Intermediate Wallet 2 received 4.854503715184017 ETH in two deposits, both on March 30, 2021, and sent 20.02 ETH in three transactions, March 19 and 29, 2021 as well as April 7, 2021, to Suspect Wallet 2 after the McNulty theft. This user Id is associated with an individual located in Nigeria.

17. SUBJECT WALLET 3, Binance user ID 18211927, belonging to or associated with MOSES OLUMIDE SOKALE, is correlated with wallet address 0x9732c9F4D781AC1b01F7A72Bb4eC4dAe7b4F1cc2. Subject Wallet 3 has received ether in six separate transactions from wallet 0xf1ee9aa010891dad45e7322c60adb85d33773f24 (Intermediate Wallet 3), totaling 4.468094444130979 ETH. Intermediate Wallet 3 received 7.5 ETH in two deposits from Suspect Wallet 2 in November and December of 2020, prior to the McNulty theft. Intermediate Wallet 3 received 2.01 ETH from Suspect Wallet 1 on February 21, 2021 after the McNulty theft. This user Id is associated with an individual located in Nigeria.

18. The contents of the SUBJECT WALLETS were seized on May 24, 2022, subsequent to a Warrant to Seize Property Subject to Forfeiture dated April 15, 2022, and executed April 18, 2022, from Binance Holdings Limited, located in Grand Cayman, Cayman Islands and are currently being held in the FBI Evidence Room at 1501 Dowell Springs Boulevard, Knoxville, TN. 37909. Based on the foregoing information, I believe there is probable cause that the contents of the SUBJECT WALLETS are proceeds from wire fraud and/or involved in money laundering.

19. Based upon the foregoing information, it appears that SUBJECT WALLETS contain funds constituting or traceable to proceeds of violations of 18 U.S.C. § 1343. As a result, the SUBJECT WALLETS are subject to civil forfeiture by the United States, pursuant to 18 U.S.C. § 981(a)(1)(C). Moreover, the SUBJECT WALLETS are involved in violations of 18 U.S.C. § 1956. THE SUBJECT PROPERTY is further subject to civil forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(C) and 981(a)(1)(A), on the grounds that the SUBJECT WALLETS contained in the above-listed accounts constitute proceeds that are directly traceable to violations of 18 U.S.C. § 1956.

20. The events described herein occurred and are situated in the Eastern District of Tennessee and elsewhere. Accordingly, pursuant to 1355(b)(A) of Title 28, "A forfeiture action or proceeding may be brought in the district court for the district in which any of the acts or omissions giving rise to the forfeiture occurred".

CONCLUSION

21. The subject property constitutes proceeds that are directly traceable to violations of 18 U.S.C. § 1343 (Wire Fraud) and is subject to civil forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) and constitutes property involved in or traceable to a transaction or attempted transactions in violation of 18 U.S.C. § 1956 (Money Laundering) and is subject to civil forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C).

All of the above information is true and correct to the best of my knowledge.

FURTHER THIS AFFIANT SAYETH NOT

Jordan A. Foreman, Special Agent
Federal Bureau of Investigation

STATE OF TENNESSEE

COUNTY OF Knox

On this 25th day of September, 2023, before me, personally appeared Jordan A. Foreman, in his capacity as a Special Agent with the Federal Bureau of Investigation, to me known to be the person described in and who executed the foregoing instrument, and acknowledged that he executed the same as his free act and deed.

IN WITNESS WHEREOF I have hereunto set my hand and Notarial Seal.

Subscribed to and sworn before me on this this 25th day of September, 2023.

PAULA B. BOOKER
STATE OF TENNESSEE NOTARY PUBLIC
KNOX COUNTY

Paula B. Booker
NOTARY PUBLIC

My Commission Expires: My Commission Expires January 3, 2027